*Attorney Docket RSW920000091US1*

June 12, 2007

**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

**BEFORE THE BOARD OF PATENT APPEALS**

**AND INTERFERENCES**

In re application of Rosario Gennaro
Serial Nbr: 09/753,727
Filed: January 3, 2001
For: Method, System and Computer Program Product for Efficiently Generating Pseudo-Random Bits
Art Unit: 2131
Examiner: Matthew T. Henning

Marcia L. Doubet
For Appellant

## APPELLANT'S REPLY BRIEF

This Reply Brief is submitted in furtherance of the Appeal Brief that was filed in this case on August 23, 2006 (as amended with replacement Summary of Claimed Subject Matter on November 20, 2006), and responds to the Examiner's Answer dated April 16, 2007.

# ARGUMENTS

1. Appellant respectfully submits the following comments on the Examiner's Answer dated April16, 2007 (hereinafter, "the Examiner's Answer"). Line numbering cited herein for Appellant's claims refers to the claims as presented in Appellant's (revised) Appeal Brief dated August 23, 2006 (hereinafter, "Appellant's Appeal Brief").

2. **Regarding the 35 U. S. C. §112, first paragraph rejection of independent Claim 52**

2a. On Pages 3 - 4 of the Examiner's Answer, the carryover paragraph that begins "Claim 52 is rejected ..." discusses claim limitations from independent Claim 52. This paragraph of the Examiner's Answer admits that Appellant's specification "provides antecedent basis for the limitation of top (N-C) bits being set to zero and [sic] while the remaining C bits are random", but then states "the specification does not provide antecedent basis for (N-C) uppermost **contiguous ones of bits** being set to zero and the lowermost **contiguous ones of bits** being random" (emphasis original).

2b. Pages 12 - 14 of the Examiner's Answer discuss this rejection in more detail under the heading "Issue #1", providing an example of a binary number. In this discussion, the Examiner highlights binary digits that are set to the value of one. This is not what Appellant has claimed, and it is now apparent that a misunderstanding has occurred. The term "ones" in the claim limitation "ones of the bits" (e.g., Claim 52, lines 3 - 4 and lines 11 - 12) is intended to have its ordinary meaning in claim terminology (as when the terms "selected ones" or "particular ones" are used in claim language to refer to *some subset of any plurality*), without regard to the (coincidental) fact that a binary digit has a value of either a zero or a one.

2c. For purposes of illustration, suppose N = 16 and C = 12. (N-C) is therefore 4. If the topmost 4 (i.e., N-C) bits are all zeroes, then the 16-bit string appears as follows:

‘0000xxxx xxxxxxxx’B

where “x” represents either a value of either ‘0’B or ‘1’B. In other words, the claim limitation “uppermost contiguous ones of the bits” (Claim 52, line 3) is intended to specify which particular bits are being described from the N bits in the bitstring, namely the first 4 in this example (assuming an interpretation where the “top” or “uppermost” bits are depicted at the left). And by specifying “(N-C) uppermost contiguous ones of the bits are all set to zeroes” (Claim 52, lines 3 - 4), Appellant signifies that these first 4 bits (i.e., the first 4 contiguous bits from the 16 bits) all have a value of zero, as illustrated above. This is in contrast to the Examiner’s interpretation of the claim language, which might (perhaps) be claimed as “setting the topmost (N-C) contiguous ones of the bits [i.e., the first 4 of them, in the example] to ones”.

2d. Accordingly, Appellant maintains his position that the 35 U. S. C. §112, first paragraph rejection of independent Claim 52 is improper, as discussed in detail in **§7.1, First Ground of Rejection**, found in paragraphs 15 - 23 of Appellant’s Appeal Brief. If agreeable to the Examiner, however, Appellant is agreeable to replacing the term “ones of the bits” with “ones of the N bits” on lines 3, 4, 11, and 12 of Claim 52, as this may remove some confusion while still maintaining antecedent basis with “N-bit” – and Appellant respectfully submits that this would not change the meaning of his claim language.

3. **Regarding the 35 U. S. C. §102(b) rejection of independent Claim 52**

3a. On Pages 14 - 17 of the Examiner's Answer, the 35 U. S. C. §102(b) rejection of independent Claim 52 is discussed under the heading "Issue #2".

3b. Appellant notes that lines 4 - 8 on Page 15 of the Examiner's Answer refers to section 7.1 of Patel, citing text from this section that discusses use of a short exponent. Appellant respectfully notes that section 7.1 is found in Patel's Appendix (see section 7, titled "Appendix") and that the introductory paragraph of the Appendix states "In this section [i.e., including section 7.1] we discuss some extensions of our results which will be addressed in the future." (emphasis added). Appellant also respectfully notes that the second paragraph of Patel's section 7.1 begins by stating "Although the number of bits generated per iteration [of the disclosed generator] is large, each iteration involves a large exponent ..." (emphasis added). The second sentence of this second paragraph then states "Instead [of using large exponents], we could start with ...", and continues with the text quoted on lines 5 - 7 of Page 15 of the Examiner's Answer. Appellant interprets this to mean that Patel is stating that his disclosed generator (as discussed in the body of his paper) could be changed from using large exponents to using short exponents as discussed in his Appendix under the introductory text of "some extensions ... which will be addressed in the future" (see Section 7, introductory sentence). In other words, Appellant interprets this "short exponent" discussion in section 7.1 as Patel explicitly stating that using a short exponent is an "extension[ ] of our results" and that this extension "will be addressed in the future".

3c. Appellant also respectfully notes that Patel then states, after discussing short exponents on lines 7 - 9 of section 7.1, that changing his disclosed generator to use short exponents instead of large exponents "raises some interesting questions" (see line 10 of section 7.1, emphasis added). He then presents Question 10 and Question 11 that are "raised" due to changing to a short exponent. In particular, Question 10 is phrased by Patel as "Will this speed [that results from changing to a short exponent] impact the security of the generator?".

3d. Appellant respectfully submits that because Patel explicitly states (1) that use of a short exponent (as discussed in section 7.1) is an "extension[ ] of our results which will be addressed in the future" (as stated in section 7, emphasis added), (2) that "This raises some interesting questions" (section 7.1, line 10), and (3) that one of the questions raised is whether the security of the generator would be impacted (Question 10), then a fair interpretation of this text is that Patel apparently believed that the security of his generator would be impacted if short exponents were used instead of large exponents – otherwise, he would not raise that as an "interesting question" for addressing in the future. Accordingly, Appellant respectfully submits that Patel did not place the allegedly disclosed use of short exponents in the possession of the public, and that his paper is therefore not enabling as to the use of short exponents.

3e. Lines 9 - 11 on Page 15 of the Examiner's Answer state "... both the generator of the instant application, and that of Patel, as disclosed in Sections 5 and 7.1, are the same generators ...". With regard to this discussion, Appellant reasserts his contention that Patel's explicit statements from his Appendix, as discussed herein in paragraphs 3b - 3e, indicate that Patel did not place the allegedly disclosed matter in the possession of the public, and that his paper is therefore <u>not enabling</u> as to the use of <u>short exponents</u>. Refer also to Paragraph 45 of Appellant's Appeal Brief, where this has been discussed previously.

3f. Appellant respectfully submits that the statement on lines 1 - 2 of Page 17 of the Examiner's Answer appears to take statements in Paragraph 17 of Appellant's Appeal Brief out of context. In Paragraph 17 of Appellant's Appeal Brief, Appellant is attempting to explain that it is unclear which claim element from Claim 52 is being discussed, because there is no claim element containing the word "setting". This discussion in Paragraph 17 does not negate the fact that there are claim elements containing the word "set" (see lines 4 and 12 of Claim 52, for example).

3g. Lines 4 - 6 on Page 17 of the Examiner's Answer indicates that the citation to Page 313, lines 22 - 27 of Patel is to be replaced with a citation to Page 316. Again, Appellant respectfully submits that the text on Page 316 is found under Patel's introductory text of "some extensions of our results which will be addressed in the future", as discussed above in paragraphs 3b - 3d, and that this discussion is therefore not an enabling reference.

3h. Accordingly, Appellant maintains his position that the 35 U. S. C. §102(b) rejection of independent Claim 52 is improper, as discussed in detail in **§7.2.1) Rejection of Independent Claim 52**, found in paragraphs 27 - 32 of Appellant's Appeal Brief.

4. **<u>Regarding the 35 U. S. C. §102(b) rejection of independent Claim 13</u>**

4a. On Pages 17 - 22 of the Examiner's Answer, the 35 U. S. C. §102(b) rejection of independent Claim 13 is discussed under the heading “Issue #3”.

4b. Firstly, Appellant apologizes for an inadvertent misstatement in Paragraph 36 of Appellant’s Appeal Brief. In the first sentence thereof, Appellant referred to “n-c” bits that are produced by an iteration of Patel’s generator and to “‘c’ of those bits” (emphasis added). In Appellant’s claimed invention, the C bits are separate from the (N-C) bits (see Claim 13, lines 8 - 9, for example), and thus the suggestion in Paragraph 36 that the “c” bits should be some subset of the “n-c” bits was an inadvertent misstatement. Furthermore, Appellant respectfully submits that this discussion in Paragraph 36 should have explicitly specified that the “producing” described therein is a reference to section 5 of Patel (see section 5, lines 4 - 5), and that this discussion in Paragraph 36 of the “c” bits not being disclosed as a “... ‘provided input value’ is used ‘as a short exponent ...’ ... ” is also discussing the teachings from section 5 of Patel. The subsequent Paragraph 37 of Appellants’ Appeal Brief then discusses Patel’s section 7.1 and, as discussed above in paragraphs 3b - 3e and 3g, Appellant reasserts his contention that Patel’s text from section 7.1 indicates that Patel is not enabling with regard to using short exponents. (See also section 7.1, lines 12 - 18 of Patel, “Note that when we restrict our exponents ...”, where Patel discusses security issues that he apparently believes may arise through use of short exponents.)

4c. Accordingly, Appellant maintains his position that the 35 U. S. C. §102(b) rejection of independent Claim 13 is improper, and such position also applies to independent Claims 25 and 39, as discussed in detail in **§7.2.2) Rejection of Independent Claims 13, 25, and 39**, found in paragraphs 33 - 46 of Appellant's Appeal Brief.

5. Appellant also respectfully notes that the final sentence on Page 313 of Patel (in section 5) states – with reference to his "NEW GENERATOR" – "... output the lower n - $\omega(\log n)$ bits of $x_i$ except the least significant bit" (emphasis added). If "$\omega(\log n)$ bits" equates to Appellant's "C" bits, as stated on Page 5, line 13 of the Examiner's Answer, then this statement from Page 313 indicates that (N - (C - 1)) bits are output by Patel. Appellant respectfully submits that this is patentably distinct from his claimed approach of using (N-C) bits as output (see, for example, lines 13 - 14 of Claim 1 and lines 15 - 16 of Claim 52).

## CONCLUSION

In view of the above, Appellant respectfully submits that the rejection of appealed Claims 1 - 2, 6 - 7, 9 - 14, 18 - 19, 21 - 26, 30, 32, 34 - 37, 39 - 40, 44, and 47 - 52 is overcome. Accordingly, it is respectfully urged that the rejection of appealed Claims 1 - 2, 6 - 7, 9 - 14, 18 - 19, 21 - 26, 30, 32, 34 - 37, 39 - 40, 44, and 47 - 52 not be sustained.

Respectfully submitted,

/Marcia L. Doubet/

Cust. Nbr. for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587

Marcia L. Doubet,
Attorney for Appellant
Reg. No. 40,999